IDBrowser-2011: Identity Security within Web Browsers

Kevin Jones (kevin.jones@intel.com)
Narm Gradiraju (narm.gadiraju@intel.com)
Jack Matheson (jack.k.matheson@intel.com)

Intel chief executive Paul Otellini recently succinctly conveyed how important security has become to the computing experience:-

"In the past, energy-efficient performance and connectivity have defined computing requirements. Looking forward, security will join those as a third pillar of what people demand from all computing experiences."[1]

The Achilles heel of existing identity systems is the limited trustworthiness of the many connected devices which we use in our daily lives. In this position paper we briefly discuss progress made to increase trust and project forward to the kinds of solution that we may be able to use in the future to enhance the computing experience for all.

It is our belief that significant improvement in the security of identities can be achieved by addressing device trustworthiness as measured from the Internet.

Summary

The rise in polymorphic and man-in-the-browser attacks has highlighted how little progress we have made in securing identities. We are fast reaching an era where we cannot assume good anti-virus software and sensible password management will protect us from the majority of identity theft attacks. Instead we must focus on engineering a web in which the default security posture is an order of magnitude stronger than we see today. This will inevitably involve raising the costs of launching an attack beyond those of local software vectors alone via additional hardware or network protections.

Historically the trusted platform module (TPM) has provided the greatest hope of hardware protected security. In restricted cases it has indeed been successful in this role, for example when used with Intel TXT to secure Cloud servers [2]. However, for identities a secure model has not yet emerged which is both easy to deploy and easy to use.

To tackle this issue more directly Intel has recently announced the Intel Identity Protection Technology (IPT) [3]. IPT provides a cost effective second factor for two factor authentication that is implemented within the chipset. By using IPT, the risk of loss due to an identity theft can be greatly reduced since the use of compromised account details no longer guarantees access. This can be achieved with or without any user involvement during authentication but it does require user actions to deploy and configure.

In another example, Intel's AES-NI instruction set [4] was introduced recently to both improve performance in encryption/decryption capabilities and harden against AES attacks. AES-NI is supported by OpenSSL [5], allowing for easy adoption of low-cost hardware assisted encryption technology.

IPT and AES-NI are significant steps that can help improve the protection afforded to identities, but there are many more such steps needed to re-balance against malware and towards the greater security of identities. What is critical to these hardening steps is that there is a default security path in the browser that delicately balances ease of use with an ability to employ downstream security enhancing technologies, be they enabled by hardware, network services or some combination of both.

Device & User Trust

Trust is a prerequisite for the establishment of any relationship, but it is not a binary condition either in life or networks. Enabling, simplifying and managing the establishment of variable trust relationships that are mutually beneficial is a primary purpose of the identity ecosystem. In today's ecosystem, the individual is all too often liable for the financial consequences of a breakdown in the trust relationship, be that caused by their own error or those of an organization with which they are associated.

At Intel we are particularly interested in the first mile problem of establishing trust between a user & their devices – a problem which has received little attention in recent years, in contrast to the many models available for extending such trust to internet services. (Indeed, many of these internet scale protocols are used in our single sign-on and gateway solutions [6]) Following patterns from public key infrastructure and symmetric key models leads to the observation that a model based on two unconnected parties alone is insufficient to bootstrap any form of trust relationship. To bootstrap we need a third party that can act as a trust reference and/or protocol mediator during handshaking. In enterprise class systems we typically see a broker in this role, to mediate trust establishment between client devices and services. This broker pattern for the third-party is mainly the result of practical concerns; the broker can be deployed quickly and easily, can assist many clients and provides a valued control point for IT administrators.

In the wider context of consumer identities we do not have a natural form for the third party to take to play this role. It has become common to see consumers establish a trust relationship with many partners based on external factors such as reputation and peer recommendations, but this is only possible with a small set of organizations, and worse, bypasses the first-mile concern entirely.

So just how do I trust my devices to act on my behalf? A model encapsulated in the TPM was for the device to attest to its configuration and runtime state to an expert third party. While this is a theoretically a near ideal solution no business model has been found that could justify the rather large investment needed to make client attestation a practical option for price conscious consumers to choose.

In alternative models to the use of TPMs alone, we need to instead look to options that reduce the barrier to entry for ecosystem supporters (ideally to near zero), or at least provide obvious business models which can support any infrastructure requirements. Intel IPT here shows two desirable characteristics, it is low cost and it can act in a limited way as a trusted third-party. What it is not able to do currently is provide protections beyond two-factor authentication.

Of course it would be a very myopic view that thinks a hardware assisted approach is the only way to establish trust, but if the required third-party is not resident on the client device it must be placed in a network location accessible from the device and provide services to the device which credibly improve its security posture within a viable business model. There is no reason such a network centric model cannot be deployed although it likely has higher barriers to entry due to third party infrastructure needs.

In this view, as identity security trends towards utilization of hardware and network assistance, the browser clearly becomes the pivotal player, being both the default network portal for consumers and having direct access to hardware services should it wish to use them. A browser supported approach also has the ability to remove many usability issues that have limited adoption of other systems. What is key here is that if we want low-cost deployment options for identity security enhancing technologies we should look to abstract how they are delivered so that hardware and network supported options are both viable and create vibrant and hopefully competing business ecosystems that enable choice and encourage further enhancement.

References

[1] http://www.guardian.co.uk/technology/2010/aug/19/intel-to-buy-mcafee

[2] http://www.rsa.com/press_release.aspx?id=10754

[3] http://ipt.intel.com/welcome.aspx

[4] http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-aes-instructions-set/

[5] http://www.openssl.org/

[6] http://www.dynamicperimeter.com/